

LINUX Expert

Webmin is a powerful Linux graphical system management console, but before you undertake remote management activities you need to make sure they are secure. Jon Thompson explains how to play it safe



NOVELL IN INDIA

Novell plans to launch versions of SuSE Linux for the growing number of users who speak Malayalam, Gujarati, Tamil, Bengali and Hindi.

Rhonda O'Donnell, president of Novell in the Asia Pacific area, says the company will scale up marketing efforts in India. It recently announced an agreement to acquire 50 per cent of its Indian partner Onward Novell.

Both China and India are massive potential markets for Linux. Novell hopes these new versions of SuSE will encourage adoption of Linux over Microsoft Windows.

ALL SYSTEMS GO

Corporate web hosting company Rackspace has surveyed its users about their choice of operating system, and found a 50/50 split between Linux and Windows-based hosts.

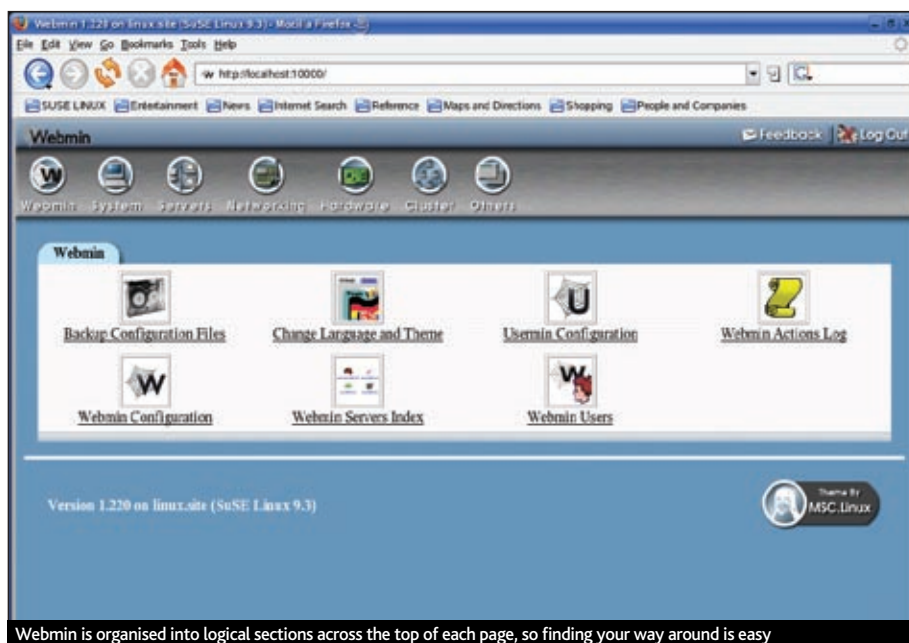
The firm found that its 13,000 customers don't consider security a major factor in choosing an operating system. Rackspace hosts sites for major corporate clients using SuSE and Red Hat Linux, as well as Microsoft Windows 2000 and Windows Server 2003.

However, 92 per cent of Rackspace's Linux users and 60 per cent of its Windows users said they feel Microsoft's systems are more vulnerable to security threats. Microsoft users also said that internal processes and people are what make an environment insecure.

NO TO WINDOWS-LINUX STUDY

The Open Source Development Labs (OSDL), home of Linus Torvalds, is likely to reject Microsoft's offer to jointly finance research into comparing Windows with Linux. The offer, made by Microsoft's Martin Taylor to OSDL head Stuart Cohen, would have seen the two companies working on what Microsoft termed "fact-based, independent" research.

After initial agreement, OSDL said it fears Microsoft could use the findings to bolster its own views. Cohen said, "I explained that Microsoft could probably find one negative line on Linux in a 100-page research report that it would spend \$10m marketing, while ignoring the other 99 pages. Why would OSDL want to participate in that?"



Webmin is organised into logical sections across the top of each page, so finding your way around is easy

Although Linux is an extremely powerful operating system, Microsoft Windows has always had the advantage of graphical system management. A common, open-source graphical system management interface that spanned mainstream Linux distributions would be a great asset to Linux. It would be even better if this interface could be accessed remotely and securely. Fortunately, this already exists in the form of Webmin.

Written and maintained by Jamie Cameron, and supported by a small army of open-source developers, Webmin currently works with more than 70 distinct Linux distributions, including the versions developed for Sony's PlayStation 2 and Sun's Solaris operating system. No matter which flavour of Linux you use, Webmin will provide you with graphical access to every configuration parameter you need in order to manage your systems. Any remote management activity is open to security risks, however. In this month's *Linux Expert* we'll look at how to secure Webmin for use over a local network, a remote private link and even the internet itself so that you can explore its extensive capabilities in safety.

Hidden from the user, the basis of Webmin is a simple web server, written in Perl for portability and dedicated to providing a graphical user interface for sophisticated scripts, called modules, that hook into various parts of the operating system as well as the sub-systems and servers that run on top of it. This web server runs independently of Apache and exists only to support Webmin. To perform a basic installation,

you just need Perl 5 or later installed and the Webmin source code.

GETTING STARTED

If you install the relevant Secure Sockets Layer (SSL) software before Webmin, you can use the HTTP's protocol automatically for a more secure connection. SSL, which we looked at in *Shopper*, September 2005, is essential for managing a server remotely over an insecure network or the net as it encrypts the traffic between you and the server.

You need to make sure you have installed both the OpenSSL libraries, including the development library, and the Net::SSL Perl module before you install Webmin. If you don't have a graphical installation tool, you can install the necessary pieces of SSL software as follows, after copying them from the distribution media. If you don't have OpenSSL and its development library, download both from www.openssl.org.

To install OpenSSL, type the following:

```
# rpm -i <OpenSSL RPM name>#
# rpm -i <OpenSSL development RPM
name>#
```

Compiling and installing it from the tarballs is just as easy. Simply type:

```
# tar xvfz openssl-0.x.y.tar.gz#
# cd openssl-0.x.y#
# ./config#
# make#
# make install#
```



Next install the Net::SSLeay Perl module. This enables Perl to access the OpenSSL library. You can obtain it from the download page at the Webmin website. To install the tarball, enter:

```
# tar xvzf Net_SSLeay.pm-<version>.
tar.gz#
# cd Net_SSLeay.pm-<version>#
# perl Makefile.PL#
# make install#
```

Installing Webmin from source is fairly straightforward too, but installing it from the RPM package is even easier. Whichever method you choose, download the latest release from www.webmin.com/download.html. Here we use release 1.220-1.

To install the RPM, enter:

```
# rpm -U webmin-1.220-1.noarch.rpm#
warning: webmin-1.220-1.noarch.rpm: V3
DSA signature: NOKEY, key id 11f63c51
Operating System is SuSE Linux
Webmin install is now complete. You
can log in to https://localhost:10000/
as root with your root password.
```

To build Webmin from scratch from the source tarball, download it into the /tmp directory on your system and enter the following commands to unpack and build it:

```
# gunzip webmin-1.220-1.tar.gz#
# tar xf webmin-1.220-1.tar#
# cd webmin-1.220-1#
# ./setup.sh /usr/local/webmin#
```

```
*****
* Welcome to the Webmin setup script, *
*           version 2.220-1           *
*****
```

Webmin is a web-based interface that allows Unix-like operating systems and common Unix services to be easily administered.

Installing Webmin in /usr/local/webmin-2.220-1 ...

```
*****
```

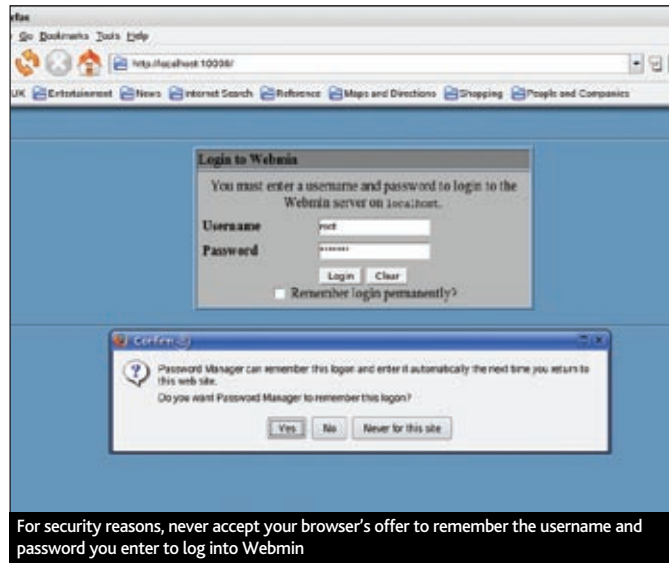
Webmin uses separate directories for configuration files and log files. Unless you want to run multiple versions of Webmin at the same time you can just accept the defaults.

You will then be asked a series of questions, including whether or not you want to use SSL (you do) and if you want Webmin to run every time you start the computer.

On some systems, gunzip is not installed by default. In this case, you should be able to use gunzip instead. Whichever method of installation you use, Webmin should start automatically and at system boot time. You can make sure it is operational by using the associated startup script, stored in /etc/init.d:

```
# /etc/init.d/webmin status#
Webmin (pid 6799) is running#
```

This script can stop, start, restart and check the



status of Webmin in the same way other server control scripts do, using the parameters 'stop', 'start', 'restart' and 'status'. To test the installation, open a web browser and enter <http://localhost:10000/> into the address bar. This works in all browsers and makes them connect to the local web server over port 10000, rather than the usual port 80. If everything is OK, you'll see the blue Webmin login screen.

After installing Webmin, we noted a curious glitch in the onscreen instructions. The message at the end of a successful RPM installation says that you can log in using HTTPS, regardless of whether you have SSL installed.

PASS MASTER

Log in to Webmin using the credentials for the system's root account. If you're accessing Webmin on a remote machine, you need to use the password for the remote root account rather than the local one. As mentioned earlier, Webmin accesses Linux's configuration files, and this includes the remote /etc/passwd.

At this point, some browsers will ask if you want them to remember the username and password you've just entered for later. Press the 'Never for this site' button on the browser pop-up. If you press the Yes button, someone could come along and simply log in to your remote server because the browser will supply the remote root password automatically. On the login page, Webmin also displays a tick box asking if you'd like it to remember you permanently; we'll show you how to make it suppress this later.

If you've installed OpenSSL, you can enable automatic SSL redirection in Webmin by logging in, clicking on the Webmin Configuration icon, scrolling down to the SSL Encryption icon at the bottom of the page that appears and clicking the radio button marked 'Enable SSL support, if available'. Click Save and Webmin redirects all subsequent traffic over HTTPS. If you haven't installed OpenSSL, the SSL Encryption page will produce a message that indicates this.

In some cases, using Webmin in SSL mode will cause your browser to complain about the SSL certificate that's bundled with the package. This is because the certificate was not issued by a recognised certificate authority. SSL still encrypts the connection, though, and you can accept the

certificate as valid. For the very security conscious, buying a real certificate from a recognised authority such as Verisign or Thawte is an option; we explained how to do this in *Shopper*, September 2005. You need to save the certificate you receive as /etc/webmin/miniserve.pem.

BORDER LINE

Once you've logged in, you'll see that Webmin is split into seven areas, as denoted by the section icons at the top of each page. These range from Webmin configuration

through to a catch-all called Others. In a busy environment you'll spend most of your time in the system, servers and, to a lesser extent, the networking areas. But it's important to set up Webmin itself securely before you start exploring. If you're not already there, click on the Webmin section icon to take you to the configuration section.

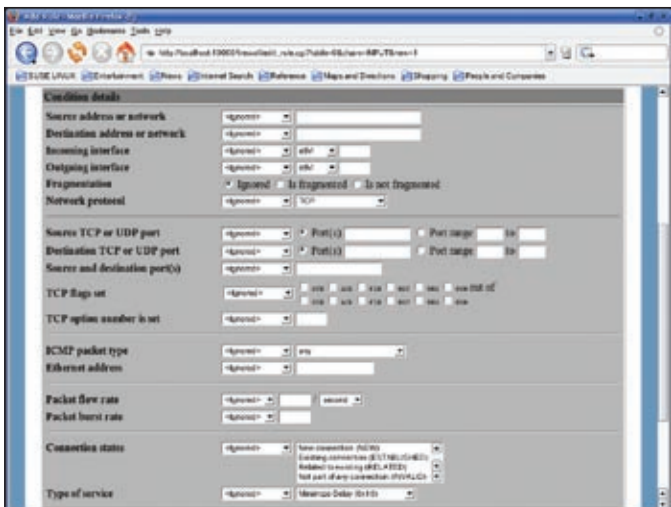
If you're going to manage several machines remotely, you'll need a consistent Webmin view across them all. Once you're happy with your setup, you can back up the configuration file and restore it to other systems on the network to save having to configure them all by hand. Click on the Backup Configuration Files icon to see the available options. You can schedule automatic backups of your Webmin configuration, but it's more likely that you'll make a change and back it up immediately. Webmin will back up all active modules as a matter of course, but you can also enter fairly sophisticated details of the destination on this page, too, including whether to use SSH to transfer the file securely to a remote server.

Although the FTP and SSH passwords entered here are displayed as dots, if you don't have OpenSSL installed the FTP password will be sent to remote servers in plain text. Because of this, it's a good idea to think carefully about the security of any link over which your machines may communicate before you decide whether to install and use OpenSSL. Restoring the configuration file ensures that you can recover from disasters quickly and keep other Webmin installations up to date.

The options are the same as those for backing up, but with a couple of additions. You can restore a configuration file stored in an arbitrary place on your network, such as on a Samba or network file system (NFS) server. The final option enables you to apply the restored configuration immediately or leave it until the next system reboot.

ACCESS CONTROL

On the Webmin menu, we can get into the meat of the program by clicking on the Webmin Configuration icon. To prevent internal users from guessing the root password and gaining access to Webmin, we need to restrict access to certain IP addresses and hostnames. Click on the IP Access Control icon to find out how. On the page that opens, you can enter a list of addresses and hostnames from which access is allowed or denied. ➔



Setting up vital but complicated sub-systems such as the Linux firewall becomes easy when the parameters are represented graphically

To allow access from your machine only, click on the 'Only allow from listed addresses' radio button and enter your hostname or IP address. Then press the Save button to update Webmin's configuration.

You can also allow or deny access from entire networks. For example, entering 192.168.0.0/255.255.255.0 will allow access from any machine on the 192.168.0 class C network that has a valid username and password, and deny it to all others. This configuration is useful in cases where you and fellow system administrators need Webmin access to servers but operate from your own subnet.

Back on the Webmin configuration page, the next task is to decide which interfaces and ports you want Webmin to listen on. This is important if, for instance, you're running it on a machine set up as a site router. It would be tempting fate to allow access to port 10000 from the internet or a demilitarised zone, so we can configure Webmin to listen for traffic only on specific interfaces. The security-conscious can change the port on which Webmin listens here, too. Remember to make a note of whatever you change this value to, or you could lock yourself out.

Another important aspect of security is to upgrade Webmin to fix any security holes that have been discovered since you performed the original installation. The Upgrade Webmin icon takes you to a page that makes this possible. You can upgrade in several ways, which include downloading any new packages yourself and installing previously downloaded upgrades from another local server over FTP, Samba or NFS, or directly from www.webmin.com. This last option is probably the easiest, as you simply press the Upgrade Webmin button.

A form at the bottom of this page gives you the option to scan for updates periodically on Webmin's home page and to install them automatically if found. While this is a great idea in principle, the accompanying text warns that if someone compromises the update server and uploads tainted code, they might take over your server and other installations all over the world. With that in mind, you should get into a routine of checking for upgrades regularly, while keeping an eye out for news reports of security breaches at the Webmin site. If there are no upgrades to install, Webmin will respond with the message: "Failed to upgrade from www.webmin.com. You

are already running the latest version of Webmin."

LOG PICKING

By default, Webmin logs the configuration changes it makes to the systems it manages. It saves these to the file `/var/webmin/miniserv.log`, and you can control how it does this. If you use Webmin heavily this file will become very large, but you don't need to keep it forever. Ticking the 'Clear log files' box and entering a time period will purge the contents of the file regularly. The default is 168 hours (one week).

By default, Webmin logs only important configuration changes. But you can log every action taken, and create a truly massive log file in the process, by clicking the 'Log changes made to files by each action' box. Ticking the 'Log resolved hostnames' box is useful in cases where you have several Webmin users and won't always know who caused which log entry. When activated, this option stores the hostname instead of the raw IP address along with the log entry.

Brute force attacks against passwords and finding logged in but unattended machines are still popular hacking methods, but you can take steps to slow or stop an attacker targeting your Webmin installation. On the Webmin Configuration page, click the Authentication icon. The subsequent screen gives a long list of behaviours you can use to frustrate a would-be attacker. One useful option involves logging you out after a period of inactivity. This ensures that if you leave your desk and forget to log out of Webmin, anyone who has physical access to your machine will need to log back in to continue. As promised earlier, you can also make Webmin suppress the automatic filling in of login details on this page. Simply untick the 'Offer to remember login permanently' box.

Before we leave Webmin configuration, it's worth mentioning that you can change the look and feel of the system by changing its user interface theme. From the Webmin configuration page, click the Themes icon. The system comes with three, but you can find more at <http://webadminmodules.sourceforge.net/?page=Themes>.

CONTROL YOUR BOOTS

It's not always obvious what programs start up when you boot up a Linux system. Webmin can come to your aid, not only listing the scripts and programs that start up at boot time but also describing what each script does. This goes a long way to demystifying the Linux boot process, so it's educational as well as handy. The screenshot on the right shows a relatively small number of items available.

You can add new items to the list too, by clicking the 'Create a new bootup and shutdown action' link. Security-conscious administrators (and we hope you are one of those) will use this screen to disable unnecessary software. For example, if you don't want to run a web server or email server, you can make sure this software does not start when the computer is turned on.

THE GREAT FIREWALL

One aspect of Linux security that causes untold worry is that of setting up a firewall. In the August 2004 issue we showed you how to set up Linux's built-in firewall and briefly gave an overview of some tools to help create its rules. But Webmin has comprehensive facilities that make this even easier.

Click on the networking section icon at the top of any page and then on the Linux firewall icon. If the firewall is disabled, Webmin gives you a few default configuration options, the option to start the firewall at boot time and a button to set up the firewall now. Click this, and Webmin will display the iptables configuration screen. If your firewall is already set up, Webmin offers to import its rule set by asking you to press a button marked 'Save firewall rules'. Press this to continue.

At the top of the page that appears you'll see three tabs, including 'Help' and 'Search docs'. The first gives an overview of how the iptables system works. The second is comprehensive, providing access to the multi-part how-to iptables documentation. It's a good idea to check these information sources when setting up or changing firewall rules if you're not sure about the available options. On this page, you can add new rule chains to your firewall configuration and new rules to existing chains by pressing the associated 'Add rule' buttons. Doing this brings up a page detailing the possible options you can apply to the rule, including flow and burst rate. But you should read the accompanying how-to documents before you add to or change your firewall configuration, especially if it protects your entire site.



Want to know what loads up when you start your PC? Webmin's Bootup and Shutdown module gives you the lowdown



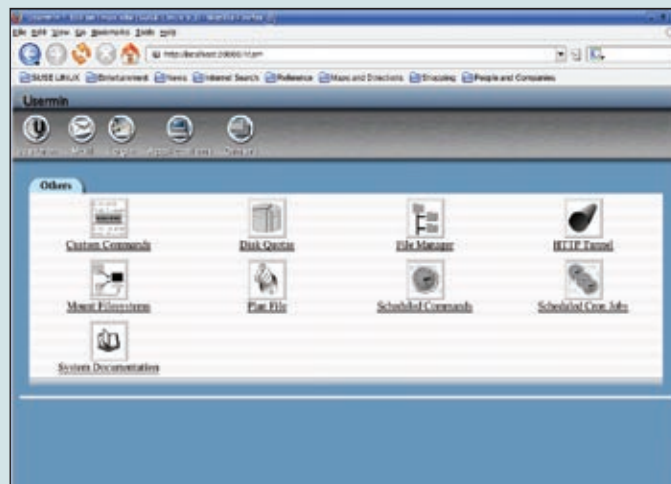
GETTING TO GRIPS WITH USERMIN

The list of features Webmin supports is extensive. You can administer Linux from the comfort of your favourite web browser, and you can also allow users to administer themselves, too. If this sounds risky, don't worry; a second tool, Usermin, can handle the task.

Click on the Webmin icon at the top of any page and then the Usermin Configuration icon. The page that opens explains that Usermin is not installed and a button appears with the option to install it from an RPM. Pressing this button downloads the latest version of Usermin from SourceForge and installs it for you.

You access Usermin using a web browser on port 20000. It looks like a cut-down version of Webmin itself, and serves as a graphical interface to frequently used programs such as mail, SSH/Telnet and a command shell. There's also a web-based file manager and a useful search facility for both the system documentation and a wider help search that uses Google.

Usermin also allows users to customise their environment, including editing their login scripts, running custom commands and even configuring their use of Pretty Good Privacy (PGP). Setting up SSH for individual users can be time consuming; Usermin allows users to set it up themselves by letting them add target hosts, keys and options. They can even schedule jobs using cron without bothering you.



You can let users take responsibility for configuring their own environment and give them graphical access to mail and other programs using Webmin's sister product, Usermin

Once you're happy with the firewall rules, you can choose to apply them immediately or reset to the last saved configuration. There are also options to start the firewall at boot time, which should be the default setting on most commercial distributions. If you think you've made a mess of the configuration and want to start again, the useful 'Reset firewall' button is ideal, as it creates a minimal rule set. If you choose not to start the firewall at boot time, it will still stay active until you reboot the system.

GRAPHICAL MANIPULATIONS

One of the great advantages of graphical system management tools such as SuSE Linux's YaST is that they make installing new software incredibly simple. Just select the desired package and away you go. Administrators who don't have access to built-in tools such as YaST can use Webmin instead.

Click on the system icon at the top of any Webmin screen and then click the 'Software packages' icon. The page that appears could save you a lot of time and frustration. It enables you to search for installed software and even remove it from the system. To see it in action, enter 'gimp' to find out if the free image manipulation package is installed. If it is, the resultant page lists not only the main package but also those that support it, such as the specific GIMP printer drivers. Selecting the relevant packages and pressing the uninstall button will remove them from the system.

Installing an RPM is just as easy. If you've downloaded a package, simply enter its path on the local machine, or to one that you can browse on the network, and press Install. You can also browse your distribution media, and even find and install packages over the internet. Pressing 'Search rpmfind.net' brings up a dialog box enabling you to search for specific packages online.

BACKUP BASICS

Everyone knows that backups are a vital part of system administration, but sometimes this realisation comes only after you've lost everything. With Webmin, however, there's no excuse for this. Click on the Filesystem Backup icon under the

system section to access the top-level options for backup and restoration features. Enter a directory such as '/home' as the source of the backup and press the 'Add a new backup' button.

This opens a page that's divided into three sections. The first details where you would like the backup to go. This can be a tape or other media device, but it can also be another machine such as a dedicated backup server. If you've installed Webmin on both servers, you can even use SSH to secure the transfer by entering a valid username and password.

In the second section you'll find the various additional backup options. A particularly useful one tries to verify that the backup archive is readable. Running a verification automatically is handy if you schedule your backups to run overnight, because it can take a while and you won't tie up a tape drive during the day, or hog bandwidth in the case of a remote backup.

The end of this section provides a useful pair of options for running scripts both before and after the backup. You might use these to perform housekeeping operations such as deleting temporary files before committing the selected directories to tape or to send yourself an email after the backup finishes to remind you to remove and label the tape in the morning.

Finally, this page contains a section on scheduling the backup job. You can use this to create a job to run later, or you can create it and run it immediately for the first time.

TAKING COMMAND

It is easy to extend Webmin's abilities. Most immediately, you can create custom commands to save time. To do this, go to the 'Custom commands' page under Webmin's Others section. Initially this page is blank except for the option to define a new command. The definition page itself is quite straightforward, but there is a potential pitfall. If you don't specify a user, you'll get an error message when you try to save the command. To define the user for the command to run as, click on the 'Webmin user' radio button or enter a valid username in the text box provided.

This page also gives you the option to make your custom command available to users of Usermin, a program similar to Webmin that's designed to help users perform tasks such as reading email; see our 'Getting to grips with Usermin' box above. Think of it as a simplified version of Webmin for users. If you want to create a command in Webmin for Usermin users, make sure you assign the correct privileges to the command. Otherwise, the users won't be able to run it.

Another extremely powerful way to extend Webmin's functionality is to download and install third-party modules, of which there are around a hundred. These can help with many tasks, including wireless network management. To install new modules, select the Webmin section, click on Webmin configuration and then Webmin modules.

There are several options here. If you've downloaded a module, you can install it directly. You can also browse the Webmin site for new official modules and SourceForge for those submitted by independent developers. You can even clone an existing module on this page. Simply select one from the pull-down list, give it a new name, select which section it should appear in and press the 'Clone module' button. This enables you to make different versions of a module available to different users, and set them up with different configuration options.

Webmin is a very powerful and easily extended Linux graphical system management console, and we've barely begun to scratch the surface of its capabilities. For instance, it can manage a complete clustering environment. For day-to-day tasks, using Webmin can mean you never have to touch the command line again. All the on-call or busy administrator needs for complete control over a wide range of systems is a web browser. **CS**

NEXT MONTH

BUILD A BRANCH EXCHANGE
We show you how to build your own private branch exchange for handling telephony.